Hastings Communications and Entertainment Law Journal

Volume 19 | Number 3 Article 4

1-1-1997

Enforcement of Use Limitations by Internet Services Providers: How to Stop That Hacker, Cracker, Spammer, Spoofer, Flamer, Bomber

Keith J. Epstein

Bill Tancer

Enforcement of Use Limitations by Internet Services Providers: "How to Stop that Hacker, Cracker, Spammer, Spoofer, Flamer, Bomber"†

by
KEITH J. EPSTEIN*
&
BILL TANCER**

Table of Contents

---

† An earlier version of this Article was presented at the *Hastings Communications and Entertainment Law Journal*'s Ninth Annual Computer Law Symposium, University of California, Hastings College of the Law, February 1, 1997. The opinions expressed by Mr. Epstein and Mr. Tancer are their own, and do not necessarily reflect those of Pacific Bell Internet Services, Pacific Telesis Group, or others. Evangeline Walsh, Tess Koleczek, and Teri Easterly assisted significantly in the preparation of this paper.

* J.D., University of Santa Clara School of Law; B.A., University of California, Davis. Mr. Epstein is Vice President & Senior Counsel, Legal & External Affairs, Pacific Bell Internet Services.

** J.D., Walter F. George School of Law, Mercer University; B.S., University of Florida. Mr. Tancer is Senior Consultant, Gartner Group, Computers Peripherals practice.

Introduction

During the early years of Internet development, the National Science Foundation (NSF) maintained an "Acceptable Use Policy" which dictated a uniform code of conduct for users of the Internet.[1] The purpose of the policy was to reserve the limited resources of the Internet for legitimate official and academic uses. When the NSF abdicated the role of controlling the use of the Internet to commercial service providers in April 1995, Internet Service Providers (ISPs) found the enforcement of a code of conduct left in their unprepared hands. Not only had the use of the Internet expanded beyond the original mandate, so too had the abuse of the Internet expanded in new and unanticipated ways. The NSF's policy was not sufficiently detailed to provide guidance to network operators who were bound by the policy to enforce it. Furthermore, the NSF did not provide any detailed illustrations regarding unacceptable uses. As a result, there is currently no uniform acceptable use policy and no agreement between ISPs and network operators regarding how to handle misuse and abuse of the Internet.

As has been the case with most technology-based legal dilemmas, the solution has not kept pace with the problem. The pace of technological change is bewilderingly fast, and it is unlikely that the law will be able to directly and quickly address issues that arise in cyberspace. In the absence of a clear body of law, ISPs will have no choice but to resort to self-help to keep the abuse and misuse of the Internet in check.

This Article is intended to be a primer for lawyers who have to deal with questions related to misuse and abuse of the Internet and

1. We dispense with a detailed discussion of the nature of the Internet, and how the Internet of 1997 compares with the Internet of just a few years ago. For purposes of this Article, a simple description of the Internet will suffice. The Internet is a network of connected computer networks, interconnecting one to another for the purpose of facilitating the passing of information in electronic format between users of information and providers of information. The Internet supports a myriad of electronic services, including electronic messaging, Usenet News (permitting users to simultaneously post messages to large numbers of other users on a wide variety of topics), file transfer (using standard protocols, users can obtain electronic files from specialized servers, including software and other interesting data), web browsing, electronic shopping, and the like. In order to use the Internet, all that is needed by the average consumer is an access device (generally, a computer, although specialized access "appliances" have recently hit the market), a modem, a telephone line, an account with an ISP, and the desired software. For a useful, albeit "legalistic," overview of the Internet, see *ACLU v. Reno*, 929 F. Supp. 824 (E.D. Pa.), *prob. juris. noted*, 117 S. Ct. 554 (1996).

who may be advising Internet Access Providers, Online Service Providers, corporate Internet users, and private Internet consumers.[2] Many of the issues discussed herein have not been finally resolved, and some may very well defy resolution. So why bother to write a primer now when the law, and the problems the law will have to resolve, are not yet clear? There are several reasons:

Prevention of Regulation. It is our experience that whenever a controversial problem is presented to the American public, and there is an outcry for a legal solution to protect the interest of a diverse population (common citizens, large corporations, educational institutions, public interest institutions, and small business enterprises), the legislative process rarely works well to address those issues. Lawyers, judges, and lawmakers tend to lack an understanding of emerging technologies, particularly the Internet, and how these new technologies are changing the way people communicate and transact business. The legislative process is one of negotiation, wherein lawmakers attempt to satisfy all constituencies. The product of the legislative process is commonly a hodgepodge of compromises that rarely generate a comprehensive and common sense solution. If the industry were to properly police itself today, the perceived need for regulation could be substantially mitigated. If ISPs and Internet users do not take responsibility for controlling abuses, the various state and federal legislative bodies and regulatory agencies will attempt to do the job for them. If the industry leaves the policing in the hands of lawmakers and judges with limited Internet experience, traditional legal principles will likely be imported to the new medium with alarming consequences. ISPs and users could find themselves subject to direct, contributory, or vicarious criminal or civil liability without actual knowledge of the crime they have committed or the tort for which they may be held liable.[3] At the risk of sounding alarmist, it is

2. At one time there was a distinction to be made between an "Internet Access Provider" and an "Online Service Provider." An Online Service Provider (OSP) offered a service which permitted customers to access stored information over a communication medium such as a telephone line, cable, or wireless network (including satellite, microwave, or mobile facilities) and combined such access with the provision of electronic content. An Internet Access Provider (IAP) offered a service that provided access to the Internet to customers, but the IAP did not engage in the provision of electronic content. Both the IAP and the OSP may have offered a suite of services, including electronic mail, but the substantial distinction was in regard to the generation of proprietary content. The distinction between the two is largely blurred today, and we use the term "ISP" to refer to both Online Service Providers and Internet Access Providers.

3. *See generally* Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards a Coherent Theory for Imposing Vicarious Copyright, Trademark, and Tort Liability for Conduct Occurring*

possible that failure on the part of ISPs to act responsibly and on their own may retard the development of the Internet.

Protection of Reputation. As will become more apparent later in this Article, an ISP's reputation for tolerance of its subscribers' Internet abuse is critical to its success in the market. ISPs and other network operators have significant powers at their disposal to sanction other ISPs who fail to take appropriate measures to detect, prevent, and terminate Internet abuse. Not the least of these powers is the ability to block traffic originating from an ISP whose service is being used to harass or intimidate others on the Internet, or whose service is used to attempt to breach network security or violate use policies and group charters. In the absence of government action or other forms of regulation, ISPs are not, and should not be, hesitant to impose sanctions necessary to protect their own subscribers and their own industry reputations. Having a reputation for fierce protection of Internet consumers will prevent the ISP from losing respectable paying customers and will discourage other unscrupulous and unsavory users bent on mischief from using that particular ISP's service to perpetrate their own nefarious deeds. A reputation for diligence in preventing abuse can even be a market differentiator for the ISP.

Avoiding Liability to Subscribers. While the extent of duty an ISP may have to a subscriber is not clear, the ISP can substantially avoid liability for its subscribers' misuse and abuse of the Internet. This can be done through the adoption of an Acceptable Use Policy, a consistent and good faith effort to enforce the policy, cooperation within the industry to detect and prevent abuse, and clear contractual language limiting the ISP's liability. To avoid liability, the ISP must clearly and unequivocally articulate the standard of conduct expected from its subscribers, and reserve the right, equally unequivocally, to terminate service in the event the subscriber violates the Acceptable Use Policy.

Over the Internet, 18 HASTINGS COMM/ENT L.J. 729 (1996). For example, some early drafts of the *NII Copyright Protection Act of 1995* included provisions which sought to impose strict liability for copyright infringement on online service providers whose systems were used to transmit or store infringing works. *See* H.R. 2441, 104th Cong. (1995).

I
Historical Perspective on Acceptable Use

In response to the need for a separate network for educational institutions, the National Science Foundation Network ("NSFnet") created an Internet backbone in 1986, providing interconnection between five super-computing centers throughout the United States.[4] The academic community received the services of the NSFnet free of charge.[5] To take advantage of this cost saving network service, a dozen regional networks were formed to connect to NSFnet.[6] Because the primary purpose of the NSFnet was to support research and educational activities, commercial uses of the NSFnet were forbidden so as not to interfere with more traditional academic pursuits.

In managing the NSFnet and the National Science Foundation articulated an Acceptable Use Policy (AUP) under the auspices of the National Science Foundation Act of 1950.[7] The Acceptable Use Policy defined two unacceptable uses of the network: (1) "use in for-profit activities unless covered by the General Principle or as a specifically acceptable use" and (2) "[e]xtensive use for private or personal business."[8] During the administration of NSFnet, several educational institutions that connected to the network extended the NSF AUP to users of their own networks in order to assure consistency across their networks. Although commercial and private use of the NSFnet was strictly forbidden, such use of the early Internet was largely ignored as long as it did not interfere with the "official" use of the network.

Several ISPs offering service before the dismantling of NSFnet used the federally funded network to carry data traffic. Several of these Internet providers included the NSFnet Acceptable Use Policy in their account "terms and conditions." Despite restrictions imposed by the NSF, commercial use of the NSFnet was growing at an estimated rate of 15-20% per month in 1990.[9]

---

4. Robert H'obbes' Zakon, *Hobbes' Internet Timeline v.2.5* (visited Apr. 6, 1997) <http://info.isoc.org/guest/zakon/Internet/History/HIT.html>.

5. KATIE HAFFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE 245-46 (1996).

6. Regional networks included NYSERNET ("New York State Educational Research Network") and CERFNET ("California Educational Research Network").

7. 42 U.S.C. § 1862(a)(4) (1994).

8. A 1992 version of the National Science Foundation Acceptable Use Policy is appended *infra* in Appendix C. The document can also be found on the World Wide Web. (visited Apr. 21, 1997)<http://ds.internic.net:80/pub/netpolicy/nsfnet_aup.txt>(June 1992).

9. Michael Hauben, *U.S. Government and Proposals on the NSF Backbone to the Internet,* AMATEUR COMPUTERIST (Summer/Fall 1993)<http://wuarchive.wustl.edu/doc/misc/acn/acn5-3.txt>.

In the early 1990's, commercial providers began building their own networks. Nationwide links built by MCI and Sprint eventually led to the decommissioning of NSFnet in April 1995.[10] To fill the gap left by NSFnet's departure, associations such as The Commercial Internet Exchange Association (CIX) were formed in 1991 as a trade alliance open to all commercial Internet carriers. All members agreed to exchange traffic at a fixed and equal cost set by the association.[11] While NSFnet catered to the research and academic community, the CIX and its commercial backbone providers provided a means of developing a public network that permitted the commercial use prohibited by the NSFnet AUP.

II
What is Unacceptable Use?

In order to fully address the concept of acceptable use of the services offered by ISPs, we will attempt to define some of the more common abuses and misuses of the Internet. One attribute of the subcultural technological revolution now sweeping the nation that both amuses and confuses is the penchant for adoption of Internet slang. We have long heard tales of "hacking" done by "hackers," but only recently have we begun to hear about "spamming," "cracking," "spoofing," "flaming," "mail bombing," and "anonymous remailing." These activities are generally prohibited by most network operators, but not well understood by lawyers and lawmakers. Common language descriptions exist for many of these activities, but the reader should be aware that there are many derivatives of each of these activities. As soon as the terms are understood a new variant is devised, or a whole new class of deviant activity is created. As discussed later, this "deviation factor" is an important part of our approach to contractual enforcement of acceptable use principles.

The following are examples of unacceptable uses of the Internet which ISP's should attempt to prohibit under the model this Article proposes:

10. *See* Nicholas Baran, et al., *The Greatest Show on Earth*, BYTE, July, 1995, at 69.

11. *Management and Operation of the NSFNET by the National Science Foundation*, 1992 Hearings before the Subcomm. On Science, Space, and Technology, 102d Cong. (1992)(statement of Mitchell Kapor, President, Electronic Frontier Foundation).

Spamming: To cause a newsgroup to be flooded with irrelevant or inappropriate messages.[12] This is often done with cross-posting to multiple Usenet newsgroups, or sending many identical or nearly-identical messages separately to a large number of Usenet newsgroups.[13]

On April 12, 1994, two Arizona attorneys, Laurence Canter and Marsha Siegel, posted an advertisement to over 6,000 Internet newsgroups.[14] The posting described a United States "Green Card lottery," a chance for non-Americans to enter a very low-odds U.S.-work-permit raffle. Canter and Siegel offered to fill in forms for a mere $95 per person or $145 a couple (without mentioning that it was free to enter). The posting of identical messages to several groups is referred to as "cross-posting" as well as "spamming." Internet Direct, Canter and Siegel's ISP, canceled its account after the deluge of complaints from Internet users rendered Internet Direct's systems inoperative.[15] In response to incidents like the one caused by Canter and Siegel, Internet providers began adding provisions to their account terms and conditions prohibiting the posting of commercial advertisements to non-commercial Usenet groups.

Mail Bombing: To send, or urge others to send, massive amounts of e-mail to a single system or person, with intent to crash the recipient's system. Sometimes done in retaliation for a perceived breach of "Netiquette."[16] Mail bombing can take many forms, from sending unreasonably large files attached to electronic mail (slowing or stopping users' ability to retrieve mail), to sending multiple copies of identical messages, or subscribing a victim to several Internet mailing lists. In August 1996, more than a dozen journalists and public

12. *The New Hacker's Dictionary* (visited April 6, 1997)<http://www.ccil.org:80/jargon>. In early 1993, several Internet users began playing an electronic form of the fantasy game "Dungeons and Dragons." The multi-user dungeons or "MUDs" were played in the form of text-based conversation or "chat." An individual who reiterated the same point several times in rapid succession, for the purpose of domineering a play session, was referred to as a "Spammer." It is believed that the choice of "spam" as the moniker for this activity is related to the British comedy troupe, Monty Python's skit depicting several Viking characters singing the praise of canned pork products. The chorus of their tribute repeats, "Spam, Spam, Spam, Spam . . . ." in repetition, and is thought to closely resemble the abusive ramblings described above.

13. This term refers to USENET News, a TCP/IP based service that is synonymous with an electronic bulletin board with over 20,000 different topic groups. Most newsgroups contain a charter that describes the topic of the group and whether commercial postings are welcome.

14. K. K. Campbell, *A Net Conspiracy So Immense* (visited April 6, 1997)<http://www.eff.org/pub/legal/cases/canter_siegel>.

15. *See infra* text accompanying note 16.

16. *The New Hacker's Dictionary*, *supra* note 12.

figures were the recipients of a mail bombing referred to as the "Great Maelstrom."[17] Victims were subscribed to over 1,000 Internet mailing lists resulting in the receipt of several thousand unwanted pieces of e-mail per day.[18]

Hacking/Cracking: The act of gaining unauthorized access to another network, computer system, or files. Cracking refers specifically to the act of breaking password protection on a network, computer system, or files. In February 1995, the case of Kevin Mitnick brought national attention to the underworld of hacking. FBI agents in their early morning raid on Mitnick's apartment seized data files containing over 20,000 credit card numbers stolen from computer systems around the nation.[19] Mitnick was also accused of hacking into computer systems at Apple Computers, Motorola, Inc., Netcom, The Well, and Colorado SuperNet.[20] As a child he gained national attention with his break-in to the North American Air Defense System (NORAD).[21]

Syn Flood Attacks: The sole purpose of a syn flood is to overburden the intended victim's systems by sending a high volume of spurious data, effectively slowing or shutting down those systems.[22] A syn flood attack was launched on the New York Public Access Networks Corporation (PANIX).[23] The PANIX attacker was reported to have sent over 200 false packets per second, rendering PANIX's service inoperable for more than a week.[24]

Forged/Spoofed Headers: Consumer Internet access accounts generally allow users to send and receive electronic mail and post articles to Usenet news. By altering e-mail and Newsreader software, users can disguise their identity to achieve anonymity, or they can assume the identity of another individual. For example, the Internet is replete with stories of a jilted lover who assumes the identity of his former girlfriend by altering a newsreader program. He then posts illicit articles assuming her identity in hopes of damaging her reputation. Forged headers are also a common method for attempting to evade law enforcement. A user who traffics pirated software by

17. David W. Methvin, *Mailbomb Maelstrom on the Net*, WINDOWS MAG., Nov. 1996, at 44.
18. *Id.*
19. Tom Abate, *How Cybersleuths Ensnared Hacker*, S.F. EXAMINER, Feb. 16, 1995, at A1.
20. *Id.*
21. *Id.*
22. *The New Hacker's Dictionary, supra* note 12.
23. Joshua Quittner, *Panix Attack*, TIME, Sept. 30, 1996, at 64.
24. *Id.*

electronic mail is likely to attempt to hide his identity with a forged e-mail address.

Flaming and Flamage: The act of emailing or posting material designed to insult or provoke.[25] One of the first incidents of flaming occured in the mid-1970s by an electronic mail discussion group called the "Header People."[26] While at times "flame sessions" are at best spirited discussions, an out of hand "flame war" can so dominate a discussion group as to interfere with others' use and enjoyment of the Internet.

"*Bots*": Automatic posting programs, or bots, originated as a method to control Internet Relay Chat sessions (or live interactive discussion groups).[27] The use of bots on IRC sessions is synonymous with the use of spamming UseNet posts to dominate a discussion group. Some Internet users have attempted to use bot technology to further the fight against Internet abuse. "Cancelbots" can be used to remove inappropriate postings to UseNet news, or used inappropriately to cancel legitimate postings.

Anonymous Remailers: While not necessarily an Internet abuse, there are several Internet sites that allow users to conduct transactions with complete anonymity. These sites were initially developed to provide secure public-private key encryption services. The anonymous re-mailer strips an incoming message of all header information and resends the message with an anonymous "from" line. Use of anonymous remailers has hindered Internet abuse verification. Some have theorized that remailers have allowed software pirates, drug traffickers, illegal online gaming operations, and child pornographers to conduct business without fear of detection.[28]

---

25. *The New Hacker's Dictionary*, *supra* note 12.

26. HAFFNER & LYON, *supra* note 5, at 215. The Header People discussion group was an unofficial mailing list devoted to the design of electronic mail headers. According to one participant, the discussions were so heated that "we normally wore asbestos underwear."

27. There are a variety of "bots" on the Internet today including Cancelbots, Chatterbots, softbots, userbots, taskbots, knowbots, mailbots, warbots, clonebots, floofdbots, annoybots, Vladbots, gossipbots, and spybots.

28. *See* Amy Harmon, *Internet Figure Pulls Plug on His Anonymity Service Technology: Supporters Say 'Remailer' Promoted Free Speech. Critics Blame It For Crime, Pornography*, L.A. TIMES, Aug. 31, 1996, at A1.

III
ISPs' Liability for Subscribers' Abuse of the Internet

From a liability perspective, the Internet is largely new ground. Few decisions help to determine how traditional concepts and laws will be applied in the online revolution. From what little law exists, and in the absence of legislative solutions, it appears as if jurists will attempt to apply "off-line" legal concepts to online torts, contracts, intellectual property rights, and electronic commerce. Lawmakers are in a quandary on how, and if, to regulate activity on the Internet. Meanwhile, businesses and individuals are moving swiftly to transact business and otherwise communicate over the Internet. It is safe to say that the law in this area will change in many ways over the next few years, but, for now, we are left to apply traditional rules to new problems.

Generally speaking, an ISP is not liable for how subscribers use the ISP's system unless it can be held directly, contributively, or vicariously liable. As a general rule, the existing case law drawn from cases involving defamation, copyright, and free speech claims suggest that an ISP may only be held responsible for the conduct of its subscribers where the ISP knew or should have known that its system was being used to damage others or to violate the law.

A. Defamation

Under the principles articulated in *Cubby, Inc. v. CompuServe, Inc.*,[29] an ISP which does not adopt the role of publisher or assume responsibility for monitoring its subscribers' postings is not liable for the statements of its users. In *Cubby*, a gossip database called "Skuttlebut" sued Compuserve and the publisher of a competing daily electronic newsletter available to Compuserve's subscribers.[30] Skuttlebut alleged that defendants published false and defamatory statements about Skuttlebut and its publisher.[31] Plaintiffs asserted that Compuserve should be held liable for statements loaded into the company's computer banks by an independent third party.[32] The court held that Compuserve took on the role of a "distributor" of information and could not be held liable absent a showing that it knew

29. 776 F. Supp. 135 (S.D.N.Y. 1991).
30. *Id.* at 138.
31. *Id.*
32. *Id.*

or should have known of the defamation.[33] A distributor is not required to be aware of everything contained in its electronic databases or which transits its electronic network.[34] According to the court in *Cubby*:

> A computer database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability . . . would impose an undue burden on the free flow of information. Given the relevant First Amendment considerations, the appropriate standard of liability to be applied . . . is whether it knew or had reason to know of the allegedly defamatory . . . statements.[35]

In *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[36] a New York court reached a similar conclusion. Plaintiff Stratton Oakmont sued Prodigy, and the "discussion leader" on Prodigy's "Money Talk" computer bulletin board, Charles Epstein.[37] Plaintiffs alleged libel *per se* for statements posted to the bulletin board to the effect that the plaintiffs committed criminal and fraudulent acts in connection with an initial public offering of stock.[38] As the discussion leader, Epstein served in the capacity of a moderator, and had the opportunity to prevent the posting of the offensive message.[39] The court held that Epstein was an agent of Prodigy, and that Prodigy was the *publisher* of the offensive message because it exercised sufficient editorial control over the content of its bulletin board that it could be held liable for the statements.[40]

B. Copyright Infringement

Even in the intellectual property and copyright context, ISPs are not necessarily vicariously liable for unauthorized copies of copyrighted work that were made and stored on its computers. The most recent case on the subject is *Religious Technology Center v.*

33. *Id.*

34. *Id.* at 141.

35. *Id.* at 140-41.

36. 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), *reh'g denied*, 1995 WL 805178 (N.Y. Sup. Ct. Dec. 11, 1995).

37. *Id.* at *1.

38. *Id.*

39. *Id.* at *3.

40. *Id.* at *6-*7. Interestingly, it appears that Prodigy's conscious choice to gain the benefit of editorial control opened it up to greater liability than other networks who simply let subscribers post what ever they want, at least until someone complains. This suggests that ISPs may very well be obligated to take action once they know their network is being used in a tortious manner, or face the consequences for doing nothing.

Netcom On-Line Communication Services, Inc.[41] In February 1995, the Church of Scientology sued an ex-minister for infringement of the Church's copyrights by allegedly posting more than 100 pages of secret church material to the Internet.[42] The ex-minister's bulletin board service (BBS) and its ISP, Netcom, were accused of strict liability copyright infringement.[43] The court held that "although copyright is a strict liability statute, there should be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party."[44] The court went on to say "it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet."[45] The court left standing a cause of action for contributory infringement to permit liability if the planitffs could show that Netcom's management was (1) aware of the posting, and (2) knew it to be infringing.[46]

In *Sega Enterprises Ltd. v. MAPHIA*,[47] the court held that the defendant's acts were more participatory than those of the defendant in *Netcom*. MAPHIA was an electronic bulletin board operator who offered storage capacity on its equipment for subscribers.[48] Acting on an anonymous tip, Sega collected evidence that MAPHIA was operating its BBS to collect and distribute pirated video game software.[49] The court held that MAPHIA had knowledge of direct infringement of Sega's copyrights by its members and actually encouraged the activity so as to be held liable under the theory of contributory infringement.[50]

The distinction between the *Netcom* and *Sega* cases turns on (1) the transient nature of the storage in *Netcom*, where the ISP "acts more like a conduit," keeping an archive of files for no more than a

41. 907 F. Supp. 1361 (N.D. Cal. 1995).

42. *Id.* at 1365-66.

43. *Id.* at 1370.

44. *Id.*

45. *Id.* at 1372.

46. *Id.* at 1381. *See also* Ballon, *supra* note 3, at 766-70 (discussing the subsequent settlement of the *Netcom* case).

47. 948 F. Supp. 923 (N.D. Cal. 1996).

48. *Id.* at 927.

49. *Id.*

50. *Id.* at 933. *See also* Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993). In *Playboy*, a bulletin board operator was held liable for copyright infringement for allowing subscribers to download plaintiff's copyrighted photographs from the defendant's bulletin board.

short duration,[51] and (2) the knowledge and encouragement of the infringing activity by the system operator. This case law strongly suggests that ISPs must establish a practice of taking action when they have notice of offensive activity taking place on their service, particularly where the ISP's involvement is more than acting merely as a conduit for the offending activity.[52]

C. Free Speech

The courts have recently addressed the issue of whether the refusal of an ISP to allow a user to send unsolicited e-mail advertisements over the Internet would amount to an infringement of free speech under the First Amendment to the United States Constitution. In *Cyber Promotions, Inc. v. America Online, Inc.*,[53] the plaintiff was an advertising agency that provided "advertising services for companies and individuals wishing to advertise their products and service via e-mail."[54] AOL received numerous complaints from disgruntled subscribers and became upset with the plaintiff's delivery of unsolicited email to AOL subscribers over the Internet.[55] AOL subsequently sent a number of "e-mail bombs" by gathering all unsolicited e-mail messages sent to undeliverable AOL addresses in a bulk transmission to the plaintiff's ISPs.[56] The plaintiff filed suit against AOL, alleging that because of AOL's e-mail bombings two of the plaintiff's ISPs terminated their relations with it, and a third ISP refused to provide the plaintiff with service.[57] In its first amended complaint, the plaintiff sought a declaration that it had the right to send unsolicited e-mail advertisements to AOL members via the Internet.[58] The district court concluded that the plaintiff did not have the right to send unsolicited e-mail to AOL members and that AOL, as a private company, may block any attempts by the plaintiff to do

51. *Netcom*, 907 F. Supp. at 1372.

52. Note that the WIPO Copyright Treaty adopted by the Diplomatic Conference on December 20, 1996 creates an express exemption from copyright infringement liability where the service provider acts merely as "conduit" in the distribution of an infringing work. *See WIPO Copyright Treaty* (Dec. 23, 1996)<http://www.wipo.org/eng/diplconf/distrib/95dc.htm>.

53. 948 F. Supp. 436 (E.D. Pa. 1996).

54. *Id.* at 439.

55. *Id.* at 438.

56. *Id.* at 437.

57. *Id.*

58. The plaintiff asserted violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1994), as well as state commercial tort claims. AOL filed a counter suit seeking injunctive relief and damages. *Id.* at 437-38.

so.[59] AOL was held not to be a "state actor" under the three tests for state action enunciated by the United States Court of Appeals for the Third Circuit.[60] As a private company, AOL was free to prevent the undesirable activity by any means at its disposal.

D. Lessons Learned

It is admittedly difficult to draw a cohesive set of rules from disparate legal disciplines that will fit any set of circumstances, but that is often precisely what clients ask their lawyers to do. At the risk of oversimplifying complex legal theories, here are the essential lessons from the meager case law available today.

Based on *Cyber Promotions*, a privately owned ISP is well within its rights to exercise control over information posted in public places within the ISP's services or sent via the Internet to the ISP's subscriber. The ISP may take whatever reasonable action it deems necessary to protect itself and its subscribers from abuse. Meanwhile, the lesson from *Cubby* and *Prodigy* is that knowledge of the offending conduct, together with the opportunity to prevent or curtail such conduct, could very well give rise to a duty to act. Finally, *Netcom* and *Sega* suggest that contributory liability could attach merely from the knowledge of an offending act. This makes for a compelling argument that the ISP should take measures to protect itself and its subscribers by limiting the manner in which its service may be used by both subscribers and outsiders.

But how invasive should such protective measures be? This Article does not suggest that the ISP must take extraordinary measures to detect and prevent misuse. Indeed, an ISP is prohibited from engaging in some very invasive actions, such as monitoring e-mail traffic, under the Electronic Communications Privacy Act (ECPA).[61] Once a message is posted in a public place accessible by other subscribers or the offending message is sent to another subscriber who complains about the posting, however, the ISP is not

59. *Id.* at 445-46.

60. *Id.* at 445. The three "state actor" tests were taken from *Mark v. Borough of Hatboro*, 51 F.3d 1137 (3d Cir. 1995). The first test is the "exclusive public function" test, wherein the inquiry is whether "the private entity has exercised powers that are traditionally the *exclusive* prerogative of the state." *Id.* at 1142. The second test is whether "the private party has acted with the help of or in concert with state officials." *Id.* The third test is whether "[t]he state has so far insinuated itself into a position of interdependence with . . . [the acting party] that it must be recognized as a joint participant in the challenged activity." *Id.*

61. 18 U.S.C. §§ 2701, 2702 (1994).

prohibited from reviewing the posted material. Any expectation of privacy held by the user who posted the offending message is nullified by the posting of the message for review by others.

Because it is still not certain that an ISP will be held liable to its subscribers, to other ISPs, or to unrelated third parties for misuse and abuse of the Internet, why bother to take on the onerous task of adopting and enforcing an Acceptable Use Policy? The answer is simple. If the ISP does not *accept* responsibility to resolve disputes, responsibility will nonetheless be thrust upon it by other members of the Internet community. It will not suffice for the ISP to ignore disputes no matter how painful dispute resolution might be. ISPs which shun their duties to the community will suffer the ultimate punishment of a networked community: isolation. This means the offending ISP could easily find its subscribers' access to the resources of the global Internet blocked. Without access to the global Internet, an ISP has little or no chance of survival in the Internet access market.

IV
Enforcement Scheme

Generally speaking, there are three components to the enforcement scheme proposed in this Article. All three components serve the purpose of resolving issues of abuse or misuse of the Internet. These components, if properly implemented, can be successfully utilized by any ISP to prevent unacceptable use of the Internet:

(1) *Contractual Use Limitations*: An ISP should include in its service agreements with customers, resellers, and sales agents a set of express "Use Limitations" that generally describes *conduct* which the ISP intends to preclude;

(2) *Acceptable Use Policy*: An ISP should adopt a standard set of guidelines applicable to all subscribers, which we refer to as an "Acceptable Use Policy" or "Policy," and which provides *examples* of conduct, based on actual or known incidents, that constitute violations of the Contractual Use Limitations; and

(3) *Practices and Procedures*: An ISP should implement *practices and procedures* which assure swift identification of problems as they arise, and which promote consistent and certain application of the Policy and Use Limitations.

The success or failure of the ISP in enforcing the Policy and Use Limitations depends on the ISP taking an active, if not proactive, role

with respect to quickly identifying policy violations, investigating such violations with tenacity and professionalism, and taking immediate and decisive action. An ISP which ignores its Policy, Use Limitations, and practices and procedures, or who enforces them in an arbitrary and inconsistent manner, will most likely not be successful in defending itself from breach of contract claims arising from disciplinary action taken against subscribers who violate the Contractual Use Limitations.

The Policy should be maintained separately from the Contractual Use Limitations for several reasons. The Contractual Use Limitations document the *intent* of the parties to prohibit certain activities based on the implications to the ISP and the subscriber. As a general expression of intent, the Use Limitations provide the ISP with greater flexibility in addressing specific conduct which may not have been anticipated or possible at the time the service agreement between the ISP and the subscriber was executed, but which nonetheless constitutes a clear breach of the acceptable standard of conduct. The Policy, on the other hand, is a more specific identification of conduct which is known at any particular moment in time to be a violation of the Use Limitations in the service agreement. The Policy is a living and evolving document that contains illustrations and examples of conduct unacceptable to the ISP. The Policy illustrates for the subscriber the types of conduct considered a violation of the Contractual Use Limitations, subjecting the subscriber to disciplinary action. As the industry is in its early stages of development, so too are those who are bent on using the Internet to commit acts of mischief or abuse. Contracts that merely prohibit specific examples of prohibited conduct will quickly be out of date as abusers devise new and creative ways to carry out their mischief. An ISP does not want to amend its subscriber contract, and go through the effort of obtaining subscriber approval of a new revised agreement, every time a new form of abuse is attempted somewhere in the industry. While the service agreement is usually executed at the time the subscriber establishes service, the Policy can be posted at a conspicuous and easily reached location on the ISP's web site or can be delivered periodically to the subscriber via e-mail or other medium.[62]

62. ISPs generally use "click to accept" service agreements which the user is required to execute electronically prior to gaining access to the ISP's service. A "click to accept" agreement is commonly used with software licenses as well. The agreement is presented to the user in the form of a dialogue box displayed before the user installs or launches software, or before the user is permitted to log onto an online service. The user is told that he or she must agree to the terms

V
Contractual Use Limitations

The Contractual Use Limitations' terms should contain, at a minimum, terms that put the subscriber on notice as to the types of activities that may result in disciplinary action. Model Contractual Use Limitation language is included in Appendix A.

A. Compliance with Rules, Regulations, and Policies[63]

First, the Use Limitations should place the subscribers on notice that they are obligated to honor the rules, regulations, and policies of any Internet service or resource that they may access in the course of using the ISP's service. It is not the ISP's responsibility to republish every rule that may apply when the subscriber accesses a third party's service. It is incumbent on the subscriber to know the rules that apply in cyberspace. Similar to the duties imposed on individuals in their family life and countries in international diplomacy, it is the ISP's duty to uphold reasonable rules of its Internet neighbors. In this way, the ISP can reasonably expect other ISPs to respect its rules and regulations. Secondly, the ISP should place the subscriber on notice that such rules, regulations, and policies may be amended from time to time. The old adage that "ignorance of the law is no excuse" is alive and well in the electronic community. Thirdly, the ISP should reserve the right to take any form of disciplinary action appropriate to the infraction. The disciplinary action should be commensurate with violation; however, by reserving the right to terminate, the ISP has absolute flexibility to prevent further violations.

---

and conditions presented in the dialogue box before being permitted to use the software or service. The text of the agreement is presented in scrolling format, and the subscriber must click on an "I Accept" button before the software can be used. If the potential subscriber clicks on the "Cancel" or "I Do Not Accept" button, the software is disabled or the attempt to set up an online session is terminated. Such agreements should be enforceable. Under UCC section 2-204, a contract for the sale of goods is "made in any manner sufficient to show agreement," and under UCC section 2-206, an offer can be accepted "in any reasonable manner." In *ProCD v. Zeidenberg*, 86 F.3d 2014 (7th Cir. 1996), the United States Court of Appeals for the Seventh Circuit held that a shrinkwrap license agreement for software was binding on the buyer under the UCC. For a discussion of online contractual issues, *See* Fred M. Greguras, et al., *Electronic Commerce: Online Contract Issues*, PRACTICING LAW INSTITUTE, PATENTS, COPYRIGHT, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES, 452 PLI/PAT. 11 (Sept. 1996).

63. *See* Appendix A *infra* Part 1.A.

B. Prohibited Activities[64]

The ISP should reserve the right to take any and all action necessary to preserve the integrity of its service, up to and including termination of the subscriber's service. The reservation of rights should protect the ISP's right to take action on the first or any subsequent occurrence of prohibited activities.

The subscriber should be prohibited from using the ISP's service in a manner that violates the law.[65] While it is impossible to list each and every law the subscriber may violate, some of the more common violations relate to criminal statutes, intellectual property laws, international treaties, content-based regulations (*i.e.*, obscenity), and public utility tariffs.

The subscriber should also be placed on notice that use of the ISP's service in a manner that is defamatory, fraudulent, indecent, offensive, or deceptive, while not necessarily criminal, is prohibited.[66] For example, use of the service to publish false statements about another subscriber may force the ISP to mediate a dispute between subscribers. The ISP need not worry that disciplinary action violates free speech because, under the principles suggested by *Cyber Promotions,* the ISP's action as a private company is not state action that would subject the ISP to liability under the First Amendment.[67] Failure to take swift and decisive action in such cases will invite retaliation and may lead the dispute into full-fledged civil litigation.

Recently, people have become concerned that the Internet is becoming a haven for stalkers, child molesters, and pornographers. The extent to which this is a real concern is open to discussion.[68] These cases largely involve conflicting and confusing circumstances, and often involve subscribers who, through fear or anger, tend toward hysteria. The Use Limitations should include a prohibition against use of the service in a manner intended to threaten, harass, abuse, or

64. *See* Appendix A *infra* Part 1.B.

65. *See* Appendix A *infra* Part 1.B(i).

66. *See* Appendix A *infra* Part 1.B(ii).

67. Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436, 441-42 (E.D. Pa. 1996).

68. The case of "Filmguy" is one incident fueling the debate. Robert Jay Tashbook, using the online name "Filmguy," was charged under a federal law aimed at sexual predators who use the Internet to seek their prey. Tashbook was charged with traveling to Texas to molest a 15-year old girl he met over the Internet. John Wildermuth, *Bay Man Charged in Internet Sex Case,* S.F. CHRON., May 17, 1996, at A21. *See also* Nina Bernstein, *On Frontier of Cyberspace, Data is Money, and Threat,* N.Y. TIMES, June 12, 1997, at A1 (describing use of prison inmates to enter personal data, which has led to at least one case of cyber-stalking).

intimidate others.[69] The ISP should also investigate all such incidents carefully, and should be sensitive to the concerns of parents of young subscribers. Nonetheless, measures can be taken to prohibit and prevent such activities.

As we mentioned earlier, the ISP should zealously guard its reputation. This may require that the ISP maintain some distance from its subscribers' use of the Internet that casts the ISP in an unfavorable light. In a market as competitive as the Internet Service market, a decline in an ISP's reputation could easily translate into a corresponding decline in market share and revenue. The Use Limitations should include a catch-all provision that prohibits use of the service in a manner that tends to damage the name or reputation of the ISP.[70] Again, this is a "facts and circumstances" call and the ISP should utilize this use restriction only when it is facing the very real threat of damage to its reputation.

The market for consumer Internet Access is based on the concept that individual consumers can share common resources and thereby reduce their individual costs of obtaining access to the Internet. The ISP obtains high capacity communications resources which are then used by subscribers on an as-needed basis. The ISP's resources are necessarily limited in order to control costs, and the ISP manages these resources in anticipation that sufficient resources will be available to all those subscribers who need them at a particular time. The ISP needs to ensure that every customer has access to all the resources which were promised, but there are occasions when a subscriber's access to the Internet may be blocked by another subscriber's use or abuse of the service. Such is the case with spamming incidents, where the news servers do not have sufficient capacity to process all incoming messages at the same time. The result is that other subscribers may be unable to access their email. Therefore, it is also recommended that the Use Limitation include a prohibition against use of the service in a manner that interferes with other customers' use and enjoyment of the services provided by the company.[71]

69. *See* Appendix A *infra* Part 1.B(iii).
70. *See id.* Part 1.B.(iv).
71. *See* Appendix A *infra* Part 1.B(v).

C. Computer and Network Security[72]

Despite recent glamorization in the movies and in the popular press, the problem of computer hacking has been around as long as there have been computers and computer networks. Hacking is rarely the product of clever young computer hackers who enter networks using "back doors"[73] and devious programming skills. Most hacking is the product of system administrators and users who carelessly choose passwords, who leave passwords lying around where they can be found, and/or who forget or are too lazy to change passwords. Hacking may not even involve breaking into a computer system, but rather may be the result of lending a friend one's computer or password.

The subscriber shares in the obligation to protect his or her account from access by unauthorized persons. For this reason, two use restrictions should be imposed. First, subscribers should be precluded from attempting to break security of the ISP's or a third party's network, or to access an account which does not belong to them. Second, subscribers should acknowledge their obligation to safeguard their accounts against unauthorized access. This is to protect both the subscriber and the ISP since such unauthorized use of the service is difficult to detect. In order to maintain a reputation for reliability and integrity, an ISP which suspects that their system or an individual account has been compromised should take immediate action to prevent further intrusions.

D. Setting the Expectation of Privacy

Setting the subscriber's expectations regarding the privacy of communications is an important measure necessary for the protection of the ISP, but it also reminds the subscriber that he or she should be cautious with respect to electronic communications. It is the nature of the medium that subscribers may easily and instantly share communications they receive. If the subscriber is aware that his messages may be published, he can tailor his message to make sure it is suitable for a larger audience. Unless there is an express agreement between the sender and the recipient of electronic messages, the subscriber should expect that the recipient will share the message with

72. *See id.* Part 1.C.

73. A "back door" is a means of entering an otherwise secure computer system by way of a special access program left on the computer system by the programmer or system manager.

others.[74] The proposed Use Limitation also serves to remind the user that the ISP has no control over distribution or publication of messages received, other than the ability to deliver the message to the original addressee.[75]

The issue of anonymity on the Internet is the subject of substantial debate.[76] Many consumers will use the Internet to obtain information because there is a perception of anonymity that is inherent in the way information is exchanged in an electronic format. To a large extent, that perception of anonymity is illusory because ISP and Internet-based information providers must have at least basic routing information in order to provide the information to the user requesting it.[77] However it is possible to provide real anonymity when using the Internet, and there are existing businesses, commonly referred to as anonymous remailers, which offer anonymity as a service. Permitting subscribers to use their Internet access accounts to achieve complete anonymity should be disfavored. While it may seem appropriate, or even desirable at times, to permit anonymity to encourage free speech and to enhance the online experience, subscribers should not be permitted to use the ISP's service to avoid accountability for their actions. Again, in the interest of assuring that the subscriber is given notice of what is expected of them, the ISP may consider adding language to the Contractual Use Limitations making

74. It is a fundamental rule of "netiquette," however, that a user should not send any message which would cause embarrassment if read by her mother, child, spouse, boss, or the press.

75. *See* Appendix A *infra* Part 1.D.

76. For a fascinating discussion of anonymity and accountability in cyberspace, see Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace,* 104 YALE L.J. 1639 (1995).

77. It is more than theoretically possible to trace an individual subscriber's request for information from a particular site on the World Wide Web. At the risk of over simplifying the complexity of Internet routing, here is a non-engineering description of how web surfing works. When a subscriber dials into his or her ISP, the ISP assigns an "IP Address" to the subscriber for the duration of the session. The ISP keeps a record of the time and date the subscriber has dialed in, and records the IP Address. The subscriber then decides to "surf the web," and selects a web site (or "web page") from which to obtain information. In order for the selected web page to be displayed on a subscriber's computer, the web computer (called a "web server") must know where to send the web page. By selecting a site on the web, the subscriber is actually directing her computer to request a computer file stored on a distant web server and is providing her IP Address for the returning file. The distant web server then sends the file over the Internet to the IP Address of the subscriber. If the distant web server records the time, date, and IP Address to which the web page was sent, that information can be matched to the time, date, IP Address, and user identification maintained by the ISP.

clear that a subscriber has no right to anonymity in his or her use of the ISP's service.[78]

Likewise, an ISP should manage its business so as to be accountable, at least to a limited extent, for the conduct of its subscribers. That is not to say that the ISP should assume responsibility for its subscriber's deeds, but rather they should be prepared to assist in the enforcement of the laws by maintaining good records of their subscribers' use of the Internet. The ISP should put the subscriber on notice that it will cooperate with law enforcement officials in the investigation of complaints and that account information and other records will be provided to a law enforcement agency in response to lawful process or as necessary to protect the ISPs interests.[79] This notice reinforces with the subscriber that the service may not be used in a manner which violates the law, and that he or she will not be permitted to hide behind the ISP in the commission of illegal acts.[80] While some may feel this language will frighten away potential subscribers, it may actually provide reassurance to others who may fear that they will somehow be victimized over the Internet. There is a tension here, but the protection of good citizens and of the ISP's rights and reputation outweigh the concerns that Big Brother may, in fact, be watching.

The ISP should also put the subscriber on notice that his use of the service could subject him to jurisdiction outside his own county or state of residence. Because of the lack of geographic boundaries for any electronic interactions, the subscriber may unwittingly expose himself to liability for conduct which may be perfectly acceptable at home, but unlawful abroad. A broad notification should be sufficient to put the subscriber on constructive notice of his duty to take care so as not to break the laws of another jurisdiction.[81]

78. *See* Appendix A *infra* note following Part 1.D.

79. Under section 2702 of the Electronic Communications Privacy Act (ECPA), an entity providing remote computing service may divulge the contents of a communication to a law enforcement agency if such contents appear to pertain to the commission of a crime. 18 U.S.C. § 2702(b)(6) (1994). An ISP may also divulge contents of a communication as may be necessarily incident to the protection of the rights or property of the ISP. *Id.* § 2702(b)(5).

80. *See* Appendix A *infra* Part 1.E.

81. *See* Appendix A *infra* Part 1.F.

VI
Acceptable Use Policy

As mentioned earlier, the Policy serves to illustrate to the subscriber, by example, the types of conduct which will be considered violations of the Contractual Use Limitations and will subject the subscriber to disciplinary action. The Policy should provide examples and illustrations of prohibited conduct known to the ISP at any moment in time. It should tie back to the Contractual Use Limitation; that is, it should serve to reinforce the contract principles involved, and it should also emphasize that the listed activities are not all inclusive. The Policy serves as a guideline only, and because it is an evolving document which can be modified quickly and easily, it is flexible enough to put the subscriber on notice that likely derivatives of previously prohibited activities will themselves be prohibited. An example of an Acceptable Use Policy appears at Appendix B.

VII
Practices and Procedures

The ISP should have in place practices and procedures for detection and identification of unacceptable uses of their services. We will not attempt to write a standard methods of operation binder here, but we do suggest that an ISP establish its methods of operation with the following components:

- Detection and Identification—The best way to enhance a reputation for integrity would be to detect and identify abusive activities in their early stages. Early detection will go a long way to avoid having to deal with subscriber complaints, and will discourage subscribers from attempting to use the ISP's service to conduct themselves in nefarious ways. The ISP should have the necessary tools available to personnel charged with Policy enforcement and investigation of complaints, and make sure that they are well trained.
- Be a Good Neighbor—It is a good practice for the ISP to communicate with other ISPs with regard to their experiences with new forms of Internet Abuse. The best way to be prepared for abuses is to hear about them from other ISPs and protect against them before they happen to you.
- Complaint Procedures—The ISP should have a simple and efficient complaint resolution procedure. It should investigate complaints quickly, and report back to the complainant on the

progress of the investigation and the ultimate disposition. If there has been a violation of criminal laws, the ISP should be prepared to cooperate with the complainant to forward the incident to law enforcement officials.

• Take Decisive and Consistent Action—The ISP should not equivocate as to whether particular conduct is a violation of the Use Limitations or of the Policy. The ISP should be consistent with regard to enforcement, and be sure that the "punishment befits the crime." If a subscriber's activity is putting another subscriber in harms way, act with immediate dispatch.

• Keep Excellent Records—The ISP should keep very detailed records in two regards. First, good system usage records help ensure that individual subscribers can be held accountable for their actions. Second, an ISP should keep good records regarding the investigation of complaints. You never know when you might be called to testify in a criminal or civil proceeding.

• Cooperate with Law Enforcement and Other ISPs—It is critically important if the industry is to successfully police itself, and thereby avoid regulation, that every ISP cooperate in properly conducted investigations by other ISPs and law enforcement officials. Once process has been satisfied, the ISP should do everything in its power to assist in the investigation. Stopping abuse of the Internet, even if it is not on the ISP's network, is in every ISP's interest.

• Provide Due Process—While not required by a privately-owned ISP, it is recommended that a subscriber who is being punished for violation of the Policy have the opportunity to appeal to someone with higher authority. There need not be rules of evidence or an adversarial hearing, but there should be someone with higher authority than the investigating personnel to hear the subscriber's side of the story and who will have the final word.

• Communicate Policy—Finally, the ISP should update its Policy document as frequently as necessary, and subscribers should be reminded to review the Policy periodically. Other means of dissemination include placing Policy information in newsletters, on the ISP's web page, and in billing enclosures.

VIII
Conclusion

Acceptable use of the Internet is an area in which the law can reasonably be expected to evolve over the next few years.

Undoubtedly, lawmakers will attempt to regulate certain aspects of the New Online Frontier, and their attempts may or may not hit their marks. Judges and juries will wrestle with novel legal concepts, applying the law by allegory and analogy, and will perhaps strain traditional legal principles to fit the digital revolution. However, until there is greater clarity, ISPs are on their own, collectively and individually, to find solutions to the problems of misuse and abuse of the Internet. We believe the approach we have articulated here will assist lawyers in helping their clients make informed decisions regarding how to control aberrant behavior on the Internet, while at the same time protecting their clients' interests.

Appendix A:
Model Contractual Use Limitation Provisions

1. Use Limitations.

A. You agree to comply with the rules, regulations and policies applicable to any network, server, computer database, web site, newsgroup or ISP that you access through the Service. Any violation of such rules, regulations and policies, or the violation of the Acceptable Use Policy issued by the Company, as they may be amended from time to time, shall be cause for the Company to suspend or terminate your service.

B. The Company reserves the right, with or without notice, to suspend or terminate the service provided to you under this agreement, or to suspend, delete, or terminate any userID, electronic mail address, data file, IP address, Universal Resource Locator or domain name used by you, upon the first or subsequent occurrence of any of the following events:

(i) the service is used in a manner which constitutes violation of any tariff, regulation, treaty or law (including, without limitation, copyright, privacy, criminal, and international laws);

(ii) the service is used in a manner which is defamatory, fraudulent, indecent, offensive, or deceptive;

(iii) the service is used in a manner which is intended to threaten, harass, abuse, or intimidate others, or which is intended to violate the privacy or property rights of others;

(iv) the service is used in a manner which tends to damage the name or reputation of the Company, its parent, affiliates, and subsidiaries; or

(v) the service is used in a manner which interferes with other customers' use and enjoyment of the services provided by the Company.

C. You understand and agree that any attempt to breach the security of any computer network, or to access an account which does not belong to you, shall be considered a material breach of this Agreement, and such breach may result in suspension or termination of the Service. You further agree to immediately notify the Company of (i) any unauthorized use of your account and/or (ii) any breach, or attempted breach, of security known to you.

D. You understand that messages or documents sent by you are private only to the extent that they are not published for viewing by third persons. Private messages disclosed to third persons who chose to publish them for viewing by third persons are no longer private.

Note: The ISP may consider adding a statement that subscribers have no right to anonymity: "You further understand that you have no right to send messages anonymously in the event that the messages constitute prohibited activities pursuant to paragraph 1.B."

E. The Company will cooperate with law enforcement officials in the investigation of complaints that your use of the service violates the law. Your account information and other records will be provided to a law enforcement agency only in response to lawful process.

F. You are responsible for the contents of any information that you transmit or acquire through your use of the Service. You should be aware that you may be subject to the laws of any jurisdiction to which you transmit, or from which you receive, information. You are solely responsible for obtaining current information on any laws which may apply, including, but not limited to, copyright, trademark, and patent laws.

G. Nothing contained in this Agreement may be construed to convey to you any interest, title, or license in the userID, electronic mail address, IP address, Universal Resource Locator, or domain name used by you in connection with the Service.

Appendix B:
Acceptable Use Policy

Introductory Note

This document will be updated frequently. Please make a habit of reviewing it from time to time to stay abreast of acceptable uses of the Service.

Internet Access Use Policy

Your Internet access account allows you to access global networks through the World Wide Web, electronic mail, FTP (File Transfer Protocol), and the USENET. Your use of these services is subject to the Terms and Conditions of the Service Agreement you accepted at the time of registration for your Internet access account. This Policy is intended to provide you with a set of guidelines you must follow in your use of your account. Violations of this Policy, and therefore the Service Agreement, may result in disciplinary action, up to and including termination of your account.

In general, remember that you may not use your account:

- in a manner which violates rules, regulations and policies applicable to any network, server, computer database, web site or ISP that you access through the Service;
- in a manner which violates any law, regulation, treaty or tariff;
- in a manner which is defamatory, fraudulent, indecent, offensive, or deceptive;
- to threaten, harass, abuse, or intimidate others;
- to damage the name or reputation of the Company, its parent, affiliates, and subsidiaries;
- in a manner which interferes with other customers' use and enjoyment of the services provided by the Company;
- to break security on any computer network, or to access an account which does not belong to you.

The following is a list of guidelines for using your Internet account. This Policy is a guideline and is not an all inclusive list of prohibited conduct.

USENET Postings

Your Internet access account gives you access to thousands of USENET news groups. These USENET groups allow you to read and post articles on a variety of topics. USENET groups may be moderated or unmoderated. Groups may also have a charter that describes what posts are appropriate.

Posting commercial messages to a USENET group is a violation of this policy unless that specific USENET group has invited commercial postings in its charter. If you are unable to find a group's charter, or the charter does not address commercial postings, you must assume that commercial postings to that group are not welcome.

Posting off-topic articles or articles that are not related to that group's subject matter as defined in the newsgroup's charter is also not welcomed. Cross-posting identical postings to over five USENET groups, posting for the purpose of threatening, harassing, or intimidating USENET group users, and forging USENET post header information are also prohibited activities.

The Company does not censor or control the content posted to a USENET group. As a user of our service, you are solely responsible for the content that you publish. Upon notification that certain postings violate this policy, violate the law, or infringe on a Trademark or a Copyright of another, the Company may, at its discretion, remove offending posts from its news server.

Secure Password

Your password provides access to your individual account. It is your responsibility to keep your password secure. Sharing your password and account access with others is prohibited. Attempting to obtain another user's account password is strictly prohibited.

Electronic Mail

Your Internet access account includes the ability to send and receive electronic mail. Use of your electronic mail account to send unsolicited commercial messages is prohibited. Sending mass electronic messages or "mail-bombing" (sending mass unsolicited mail or deliberately sending very large attachments to one recipient) is prohibited. Forging electronic mail headers (addresses) is also prohibited regardless of commercial content. Use of electronic mail to harass or intimidate other users is likewise prohibited.

In the interest of maintaining network performance, users should not send unreasonably large electronic mail attachments. Users are prohibited from running programs designed to defeat network inactivity time-outs.

Illegal Activity

Any activity on the Company's network that is a violation of State or Federal law is a violation of this policy. Prohibited activities include, but are not limited to: transmitting obscene materials; intentionally spreading computer viruses; gaining unauthorized access to private networks; engaging in the transmission of pirated software; conducting or participating in illegal gambling; and soliciting for illegal pyramid schemes through electronic mail or USENET postings.

Questions?

As a member of our network community, we encourage you to use your Internet access responsibly. Should you have any questions regarding this policy, feel free to contact us at policy@_____.

Appendix C:
The NSFnet Backbone Services
Acceptable Use Policy
June 1992

GENERAL PRINCIPLE:

(1) NSFNET Backbone services are provided to support open research and education in and among U.S. research and instructional institutions, plus research arms of for-profit firms when engaged in open scholarly communication and research. Use for other purposes is not acceptable.

SPECIFICALLY ACCEPTABLE USES:

(2) Communication with foreign researchers and educators regarding research or instruction, as long as any network that the foreign user employs for such communication provides reciprocal access to U.S. researchers and educators.

(3) Communication and exchange for professional development, to maintain currency, or to debate issues in a field or subfield of knowledge.

(4) Use for disciplinary-society, university-association, government-advisory, or standards activities related to the user's research and instructional activities.

(5) Use in applying for or administering grants or contracts for research or instruction, but not for other fundraising or public relations activities.

(6) Any other administrative communications or activities in direct support of research and instruction.

(7) Announcements of new products or services for use in research or instruction, but not advertising of any kind.

(8) Any traffic originating from a network of another member agency of the Federal Networking Council if the traffic meets the acceptable use policy of that agency.

(9) Communication incidental to otherwise acceptable use, except for illegal or specifically unacceptable use.

UNACCEPTABLE USES:

(10) Use for for-profit activities, unless covered by the General Principle or as a specifically acceptable use.

(11) Extensive use for private or personal business.

This statement applies to use of the the NSFNET Backbone only. NSF expects that connecting networks will formulate their own use policies. The NSF Division of Networking and Communications Research and Infrastructure will resolve any questions about this Policy or its interpretation.